FGI's activities on R-PNT (Resilient Position, Navigation, and Timing)

Nordic Geodetic Commission, Working Group for GNSS Positioning
Session 3: Jamming and Spoofing
March 14, 2024
Helsinki, Finland

Prof. Zahidul Bhuiyan

Finnish Geospatial Research Institute

Background

- GNSS, being the backbone of any global scale navigation system, offers accurate PNT in good signal conditions but is vulnerable to jamming/spoofing

  => due to weak signal reception and open unprotected signal authentication provision

- Heavy dependence on GNSS-based PNT systems has made jamming/spoofing a growing threat

- There has been a considerable upsurge in GNSS vulnerability incidents due to the advancement of affordable software-defined radios, signal simulators, cheap availability of jammers, and a broader understanding of spoofing as an effective disruption strategy against GNSS-based applications.

Impact of spoofing on different COTS GNSS receivers

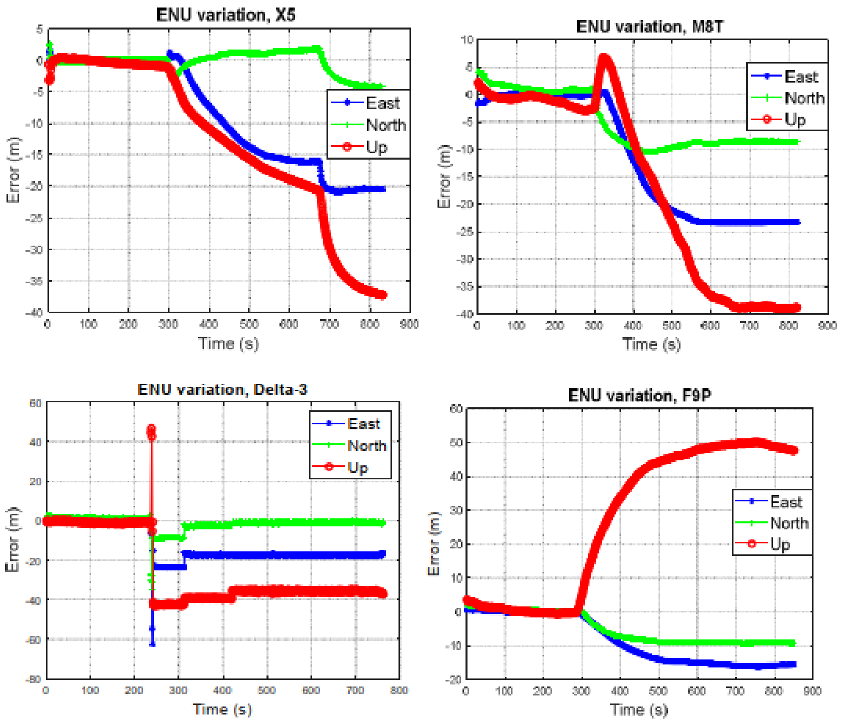
- 5 different receivers were tested under different types of spoofing attacks

TABLE VI. OVERVIEW OF SPOOFING IMPACTS ON DUTS

DUT	*Targeted spoofing*	*Untargeted spoofing*	*Meaconing*
	Spoofed?	Spoofed?	Spoofed?
M8T	YES	YES	NO
F9P	YES	YES	NO
X5	YES	NO	NO
Delta-3	YES	NO	NO
FGI-GSRx	YES	NO	NO

TABLE VII. SUMMARY OF SPOOFING IMPACT ON POSITIONING ACCURACY FOR LIVE-SKY SPOOFING ATTACK

DUT	ε_{3D}	ε_H	σ_H	ε_V	σ_V	*Availability (%)*	*Impact*
M8T	29.2	17.3	10.7	23.5	16.2	100	High
F9P	37.1	12.8	7.7	34.9	21.4	100	High
X5	21.6	12.1	8.2	17.8	12.3	100	High
Delta-3	34.8	15.9	8.7	31.0	17.0	89.6	High
FGI-GSRx	74.0	49.3	29.4	55.1	33.1	100	High



Varying spoofing impact on different GNSS receivers

Islam, S., Bhuiyan, M. Z. H., Pääkkönen, I., Saajasto, M., Mäkelä, M., and Kaasalainen, S. (2023) "Impact analysis of spoofing on different-grade GNSS receivers," IEEE/ION PLANS 2023, April 24-27, 2023, California, USA.

Interference Detection and Mitigation Techniques at Receiver level

Detection Techniques

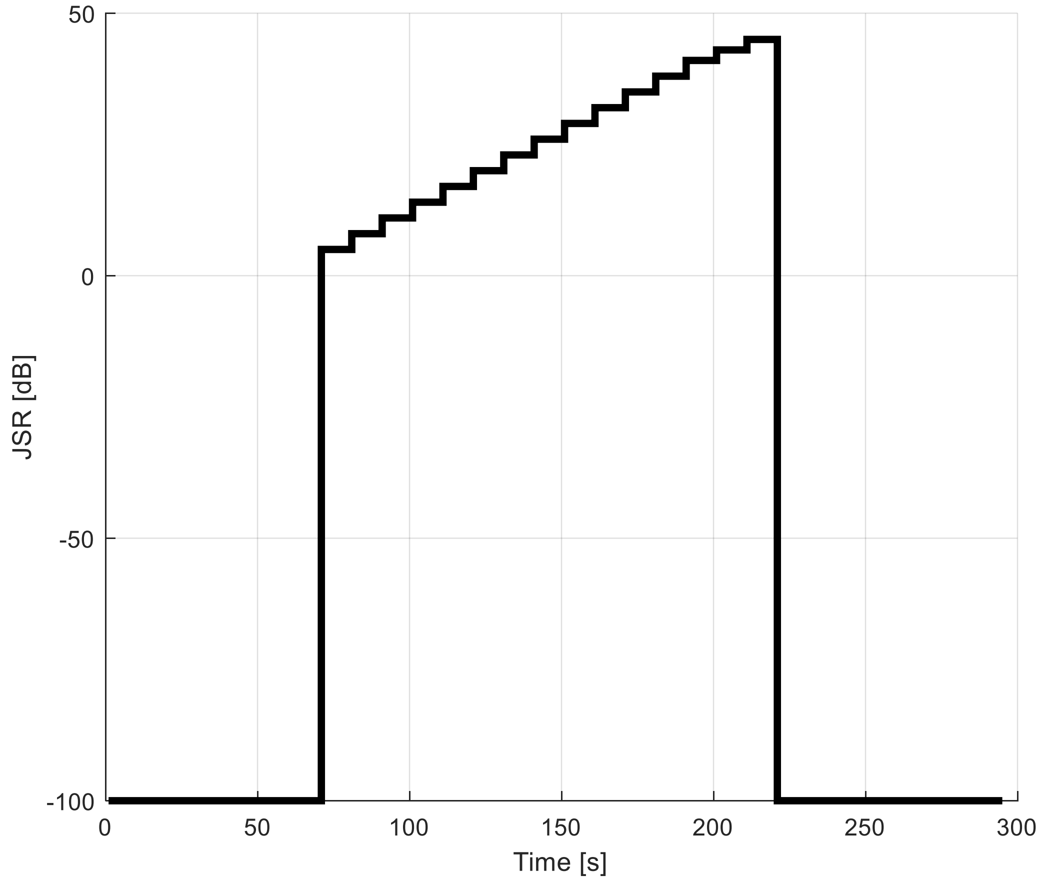
- Chi-Square testing based interference detection
- C/N_0 monitoring
- Correlation Peak Monitoring (CPM)

Mitigation Techniques

- Multi-frequency multi-constellation (MFMC) diversity
- Consistency check at navigation level

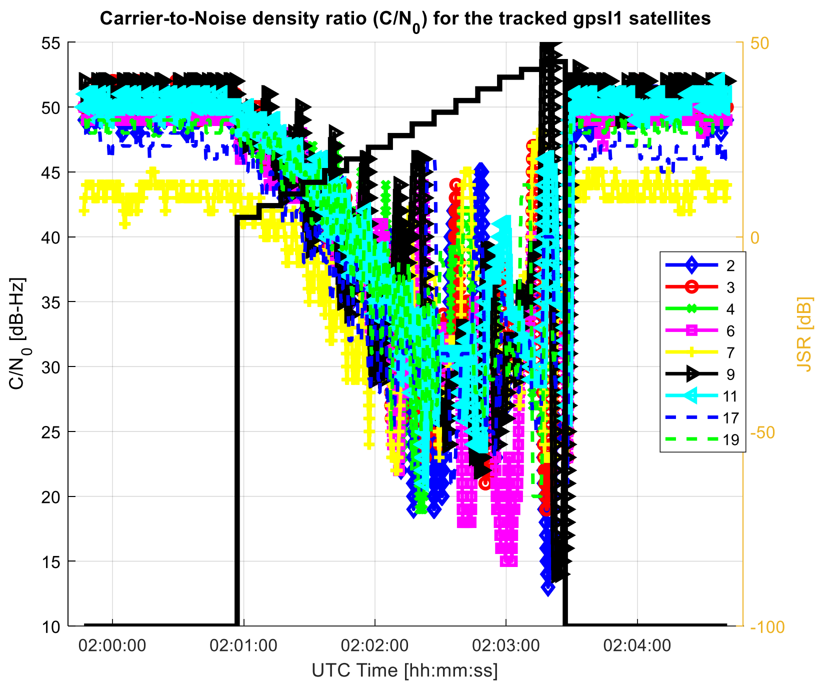
Jamming Profile

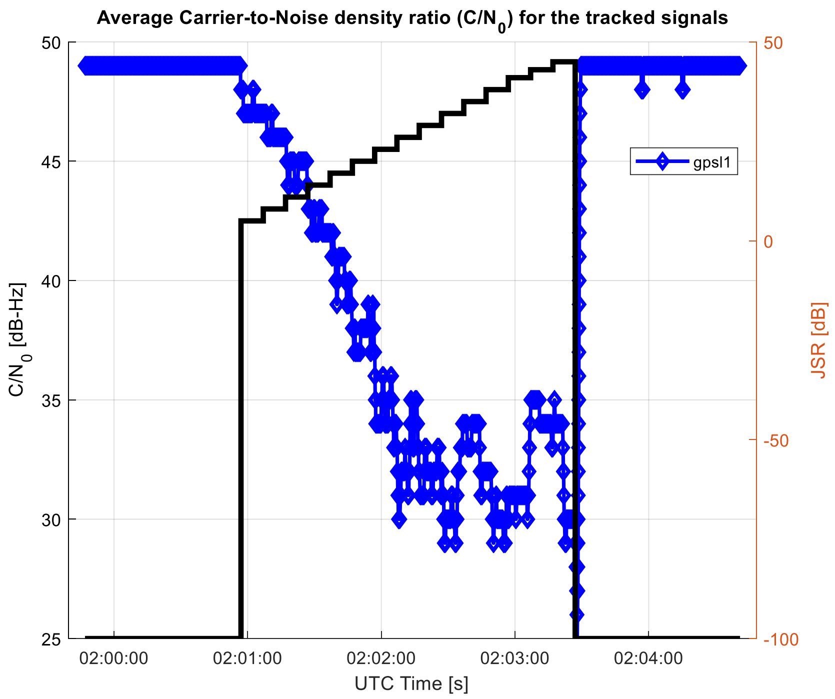
- The following Jamming-to-Signal Ratio (JSR) profile is used in all the scenarios to test jamming signals except dynamic ones.
- A 5-minute-long dataset was processed. Jamming signal was injected at 70th second, before which the receiver assumed to have decoded the navigation message.

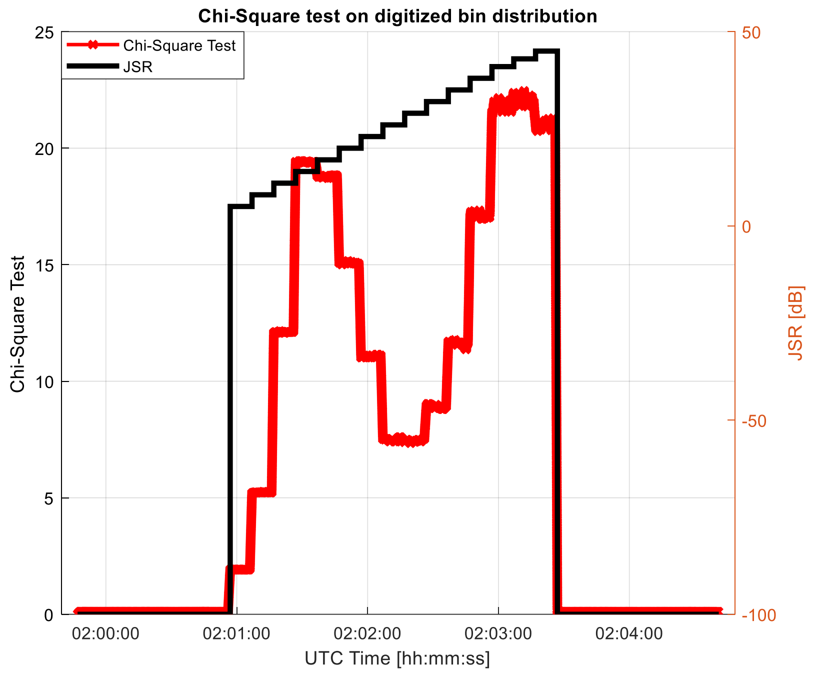


JAM-CH-S-02

Scenario ID	GNSS Constellation	DUT scope	Comments
JAM-CH-S-02: **- Static, Chirp wide (fast) in-band** **- L1/E1**	**- GPS L1 C/A** **- Galileo E1** **- GPS L5** **- Galileo E5a**	**Detection:** **AGC/IQ + C/N_0 monitoring**	**- Spiral impact at low C/N_0 levels can be seen due to the presence of strong chirp signal**

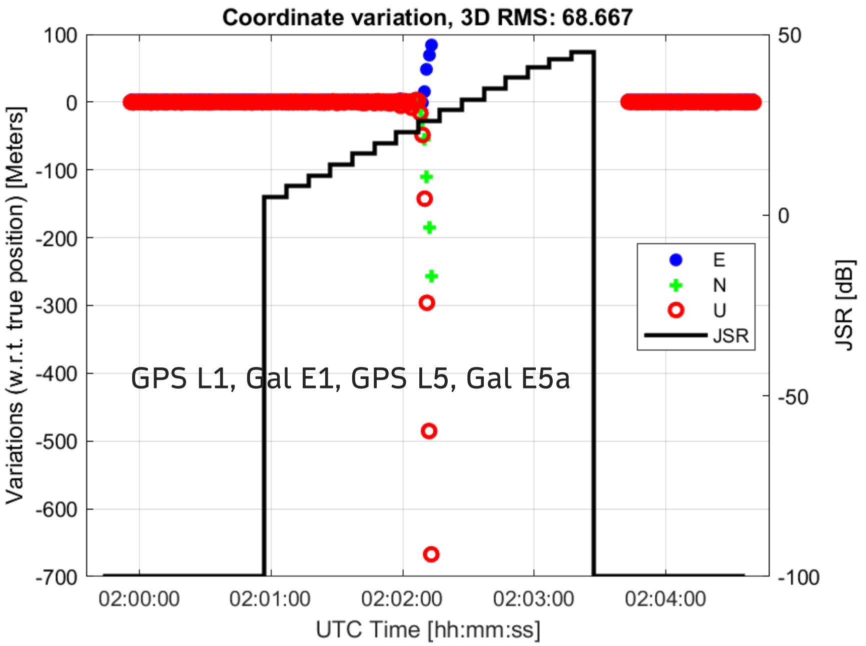




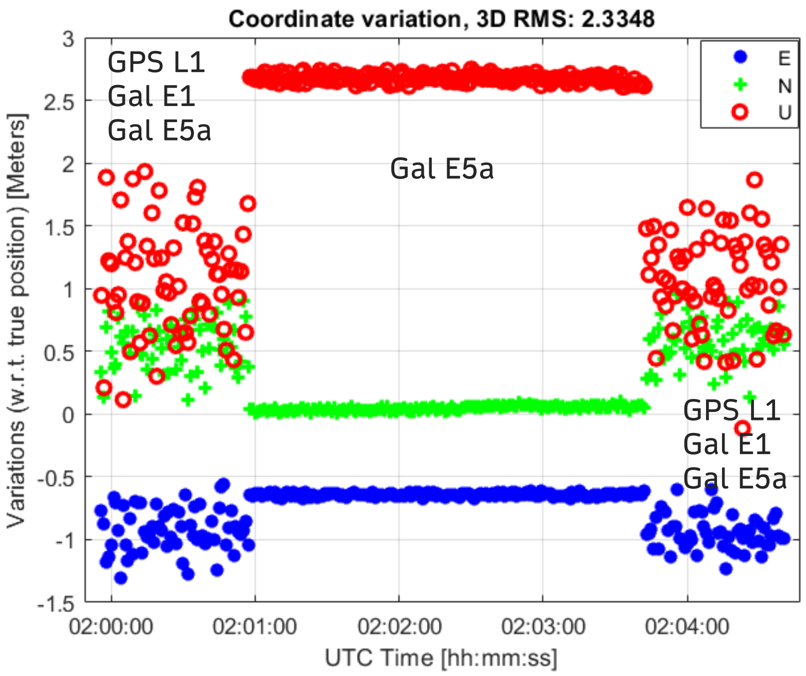


Impact of high-power jamming on L1/E1 in terms of positioning accuracy

Scenario ID	GNSS Constellation	DUT scope	Comments
JAM-CH-S-02: - Static, Chirp wide (fast) in-band - L1/E1	- GPS L1 C/A - Galileo E1 - GPS L5 - Galileo E5a	Mitigation: - Interference detected on L1/E1 - MFMC based mitigation	- MFMC diversity is applied on-the-fly based on the detection of interference at signal level for each frequency



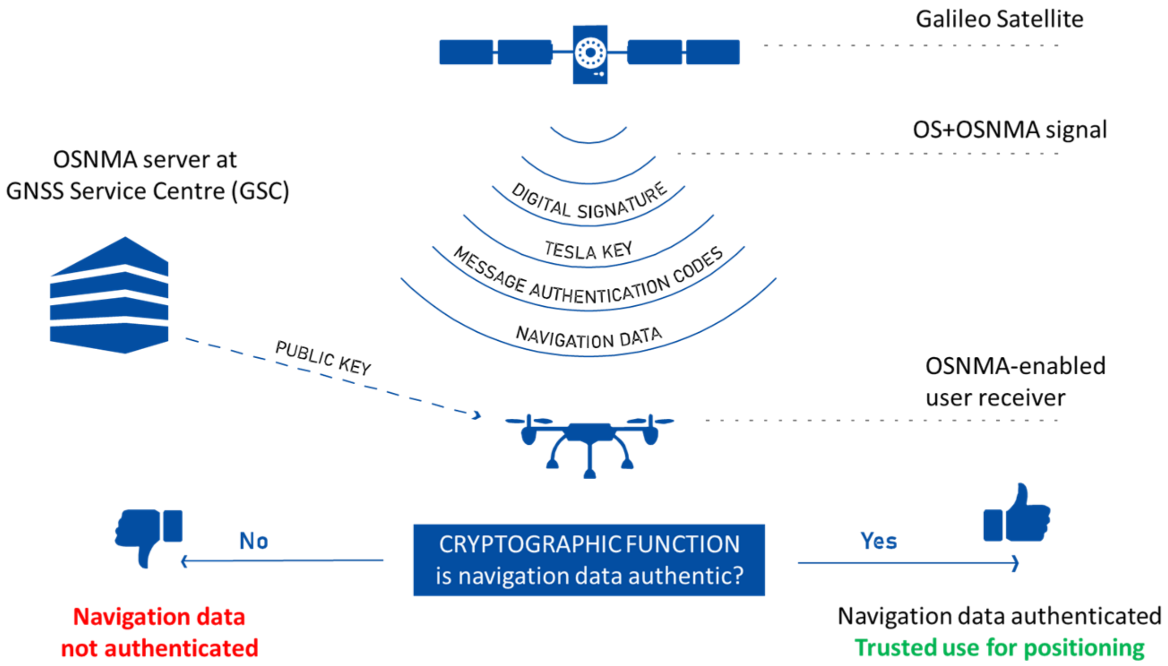
No Mitigation Applied



Mitigation Applied with AGC/IQ -based detection followed by MFMC mitigation

Open Service Navigation Message Authentication (OSNMA)

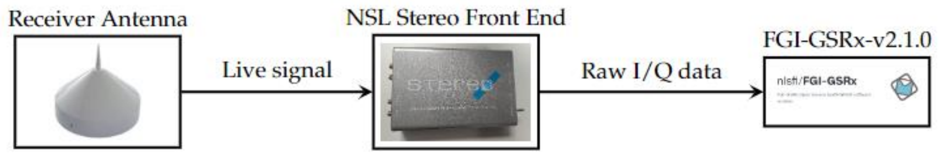
- OSNMA is a new feature of the Galileo Open Service which enables users to **verify that the navigation data** they receive **originated from the Galileo satellite** and **has not been modified.**
- OSNMA is **now available for testing** by receiver manufacturers and application developers.



Source: Joint Research Centre (JRC)

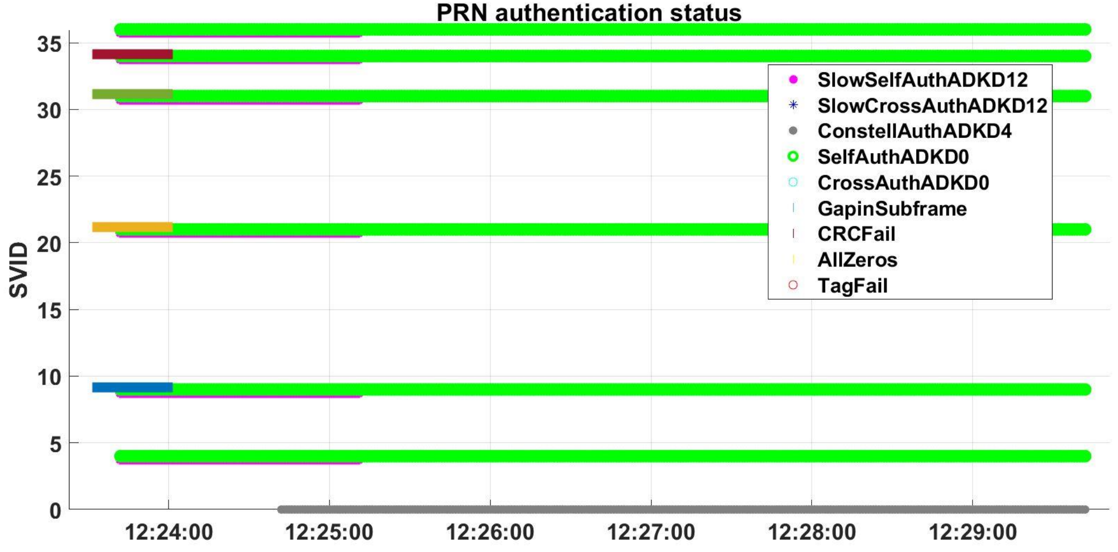
OSNMA based Position Authentication with FGI-GSRx

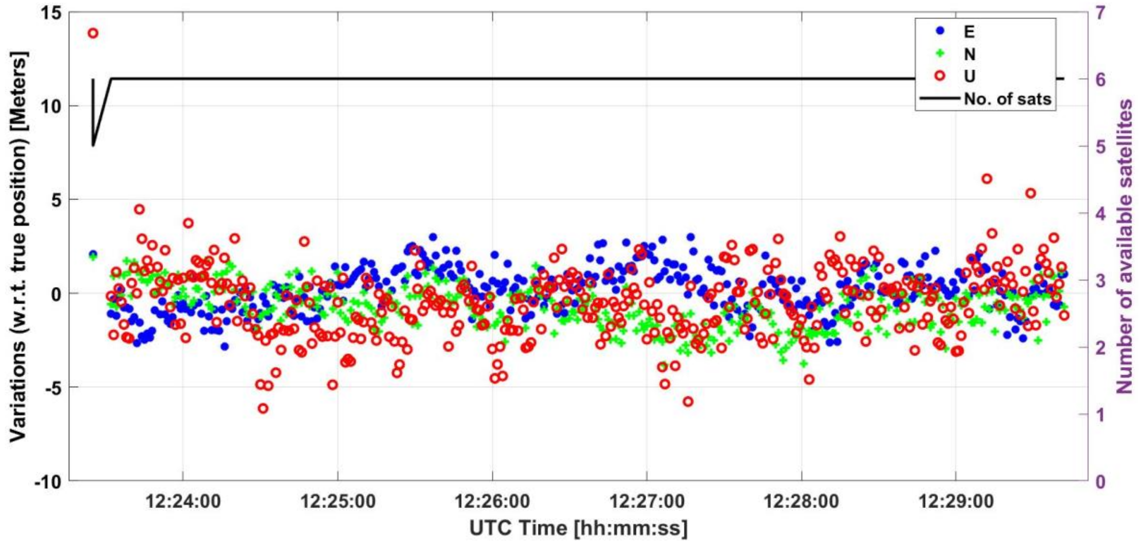
Live signal



Scenario 1: Nominal open sky clean signal

	Availability (%)	ϵ_{3D}	ϵ_V	σ_V	ϵ_H	σ_H
Auth. position	96.2	2.99	1.60	1.85	1.54	0.75





Reference: 60.182°N, 24.828°E , 47.248 m

Location: Otaniemi premises of Finnish Geospatial Research Institute (FGI) in Espoo, Finland

Galileo satellites: PRN 4, 9, 21, 31, 34, 36

Signal duration: 460 seconds (~8 mins)

OSNMA based Position Authentication with FGI-GSRx

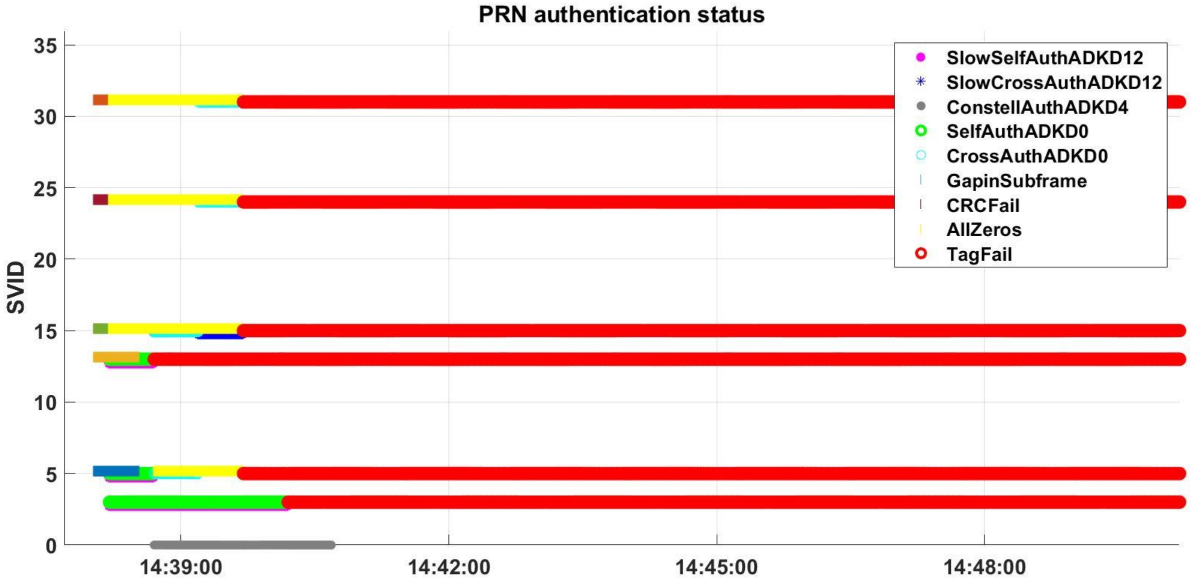
Record and Relay

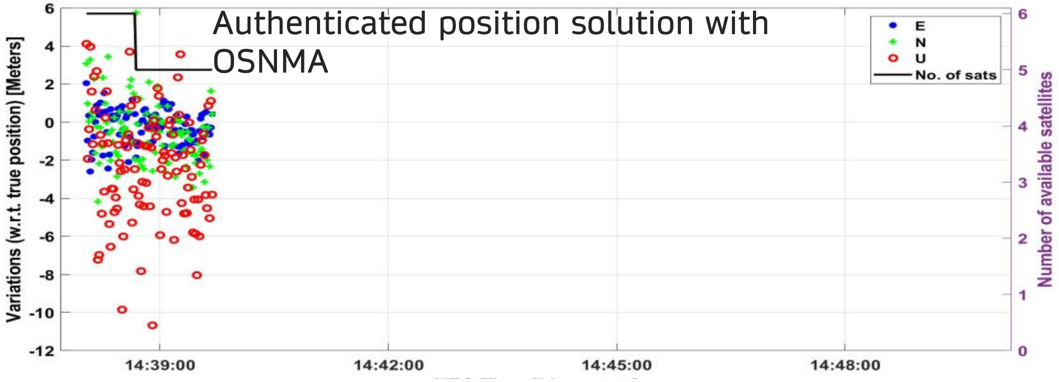
Scenario 2: JammerTest 2023 (Norway)

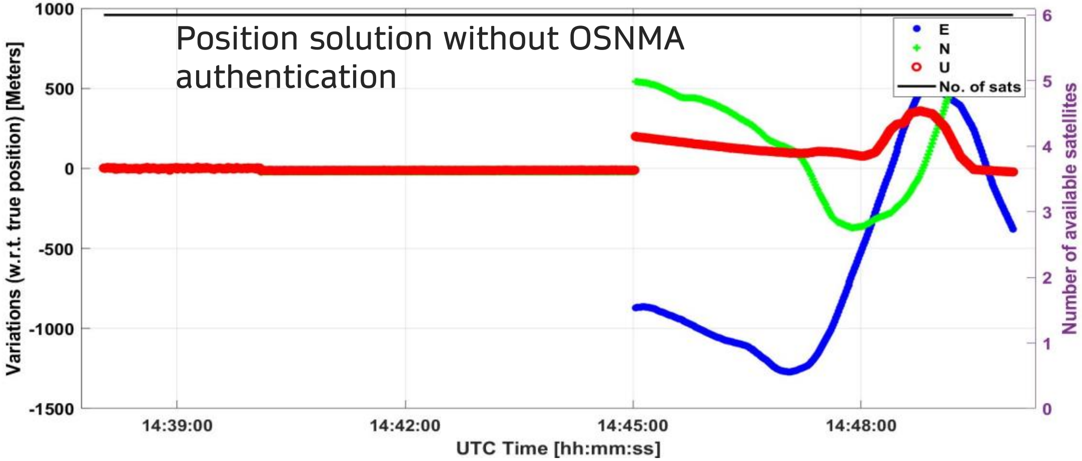
Dataset: 17.1.6 Simulated driving (route 1).

Spoofed Signals: GPS L1 C/A, L2C, L5 Galileo E1, E5

	Availability (%)	ϵ_{3D}	ϵ_V	σ_V	ϵ_H	σ_H
Auth. position	16.21	4.06	2.35	2.06	0.78	0.56
No Auth. position	100	603.55	62.62	86.08	370.21	464.96







Reference: 69.283°N, 15.998 °E

Location: (Bleik community house parking lot), Andøya, Norway

Galileo satellites: PRN 3, 5, 13, 15, 24, 31

Signal duration: 740 seconds (~12 mins)

STRIKE3 International Monitoring Network

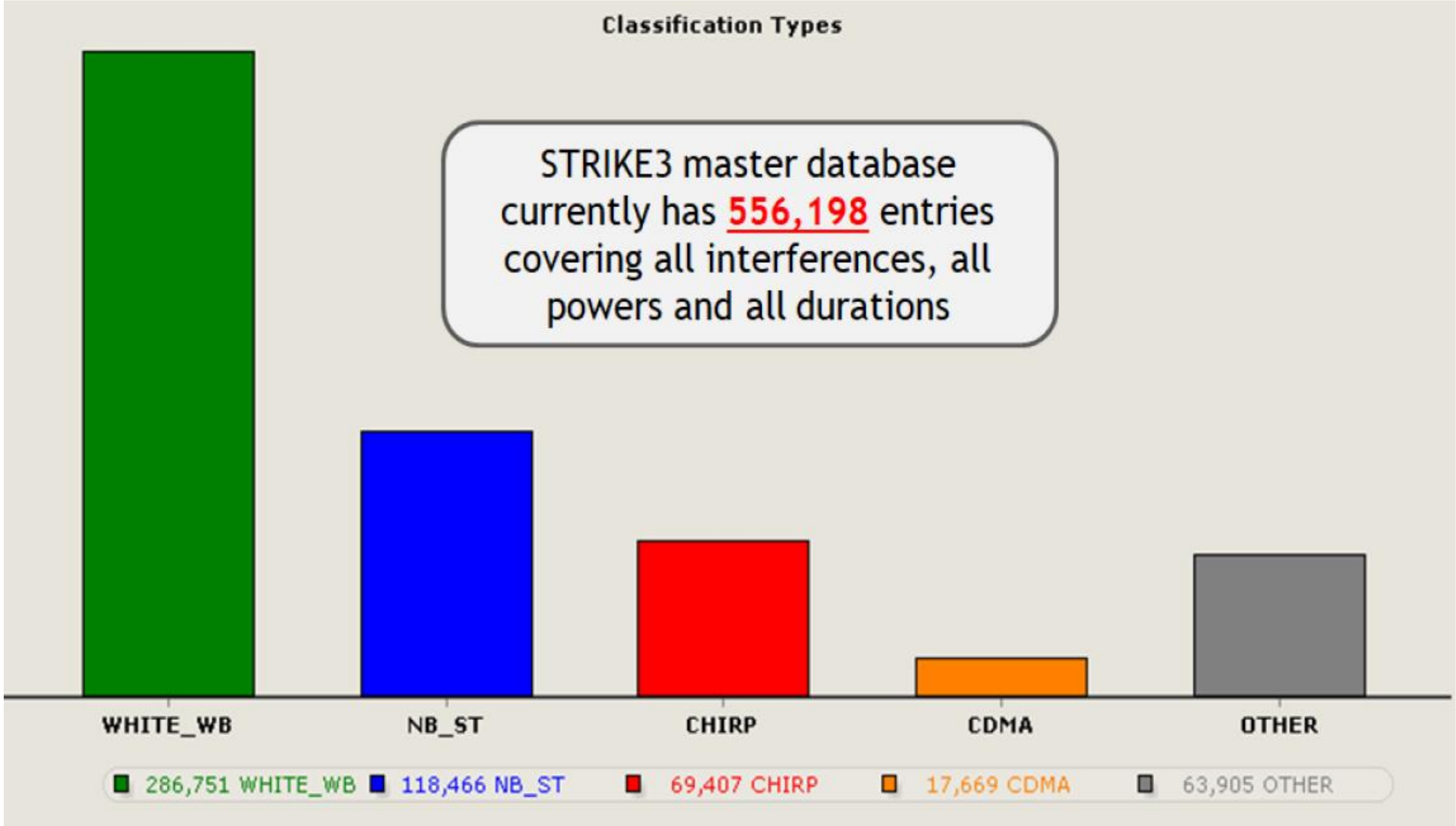
50 monitoring sites

Across the globe

- United Kingdom
- Sweden
- Finland
- Germany
- France
- Poland
- Czech Republic
- Spain
- Slovakia
- Slovenia
- Netherlands
- Belgium
- Croatia
- Latvia
- New Zealand
- Canada
- India
- Vietnam
- Thailand
- Malaysia
- Japan

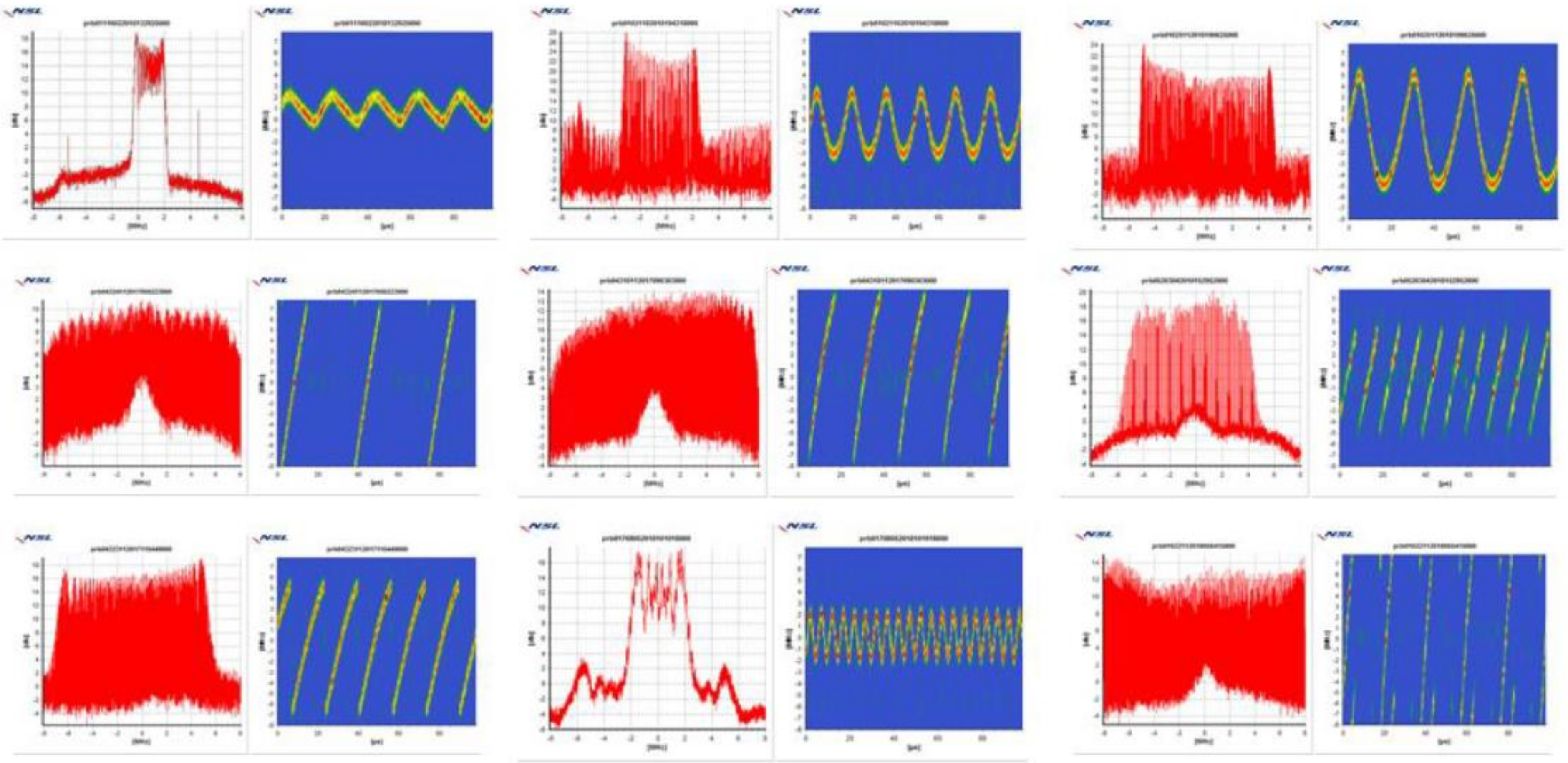
STRIKE3 participant countries each have 3+ sites. **STRIKE3 Partnering countries** have had 1 or 2 sensors. Some countries have moved a sensor to multiple locations to try to build up a bigger picture. Typical duration of a monitoring campaign at a site has been between 3 – 24 months.

STRIKE3 Master Database (1/2/2016 – 31/01/2019)



2

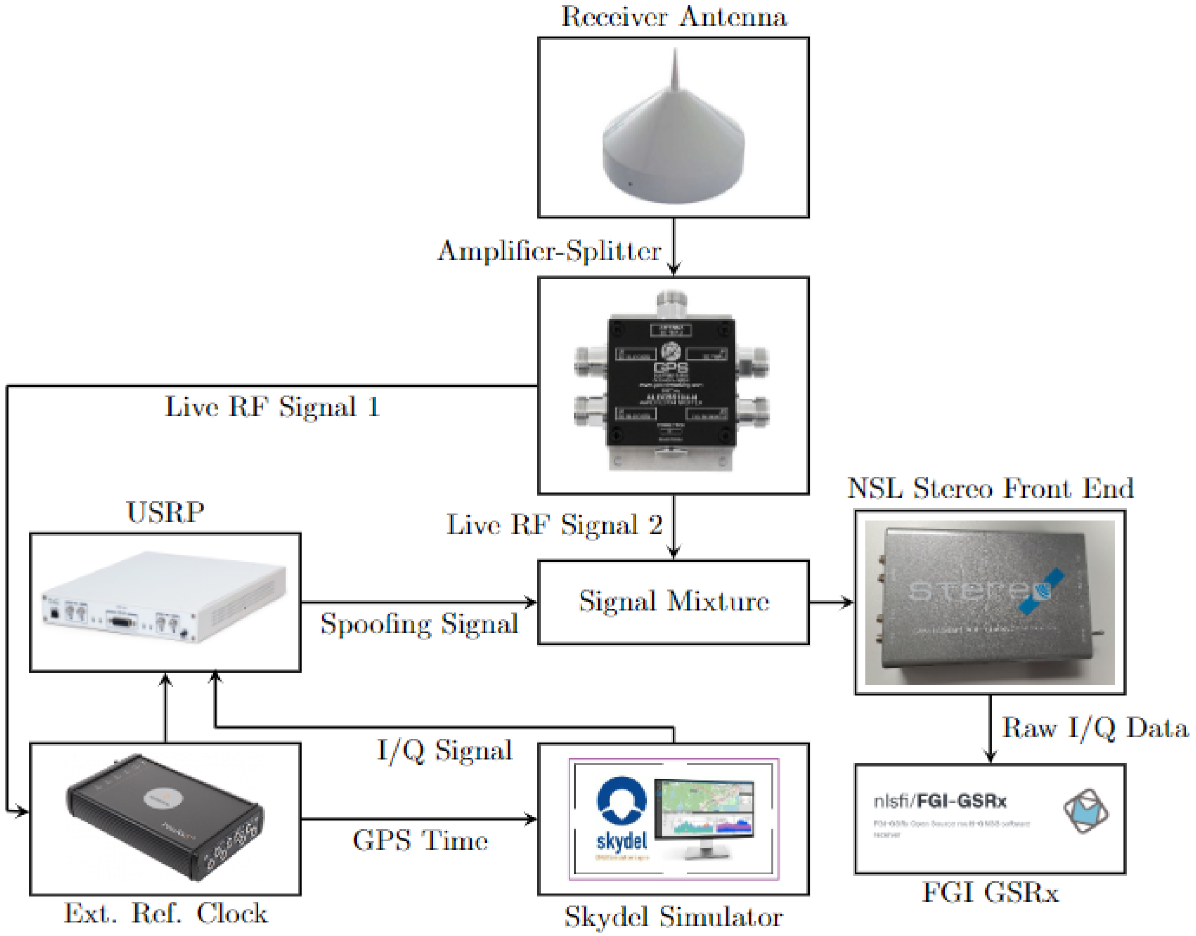
7,326 "*jammers*" that **denied** GNSS



Distance and dynamics	**Jammer** power	**Jammer** effectiveness	Local factors

Data Collection

- All the spoofing signals in the datasets are generated using the Safran Skydel software-defined GNSS simulator in conjunction with external hardware
- The simulation time is carefully synchronized with GPS time for targeted time synchronous scenarios, which is obtained from a reference GNSS timing receiver
- The live signals from the rooftop antenna and spoofing signals are combined to feed to the NSL stereo front-end to collect raw I/Q data



Saiful Islam, Mohammad Zahidul H. Bhuiyan, Muwahida Liaquat et al. An Open GNSS Spoofing Data Repository: Characterization and Impact Analysis with FGI-GSRx Open-Source Software-Defined Receiver, 12 March 2024, PREPRINT (Version 1) available at Research Square [https://doi.org/10.21203/rs.3.rs-4021306/v1]

GNSS Spoofing dataset can be found here: https://etsin.fairdata.fi/dataset/ad43952e-76e5-4000-9ebd-bc4dcb8e1cf0

Spoofing Scenarios

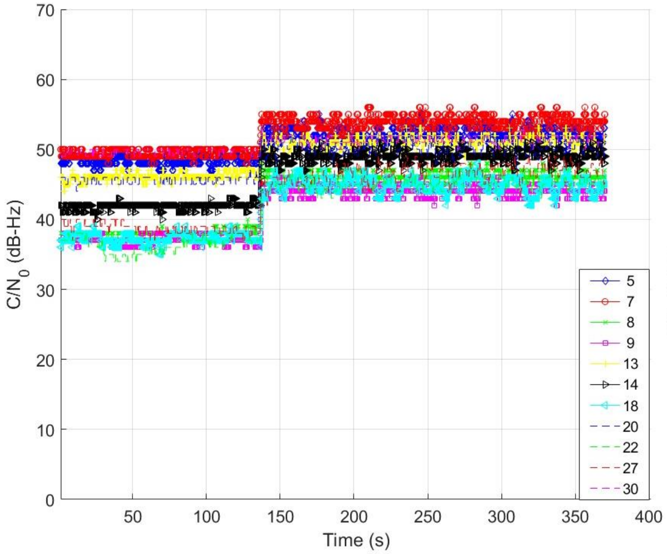
- The data repository comprise a set of four digitized recordings of live static datasets of GPS L1 C/A, Galileo E1, GPS L5 and Galileo E5a signals
- The datasets contain three types of spoofing scenarios: Targeted Spoofing (time and position synchronous), Untargeted Spoofing (time and or position asynchronous), and Meaconing (re-radiator)

Summary of spoofing scenarios

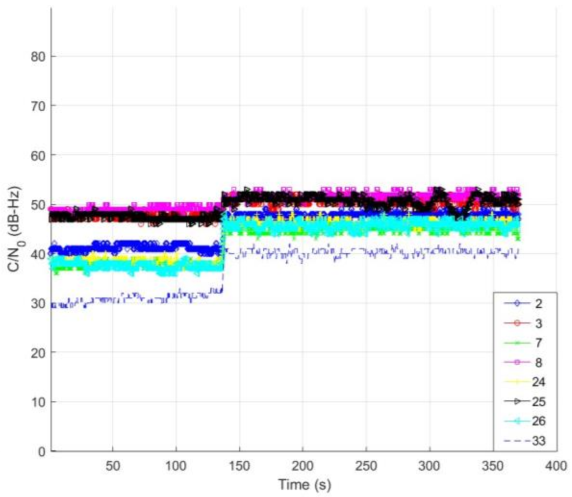
Name	Int. Position Synch	Int. Time Synch	Position Switch	Time Shift	Latest Ephemeris Injected	Spoofing Signal(s)
Targeted SFMC	Yes	Yes	Dynamic	No	Yes	L1, E1
Targeted DFMC	Yes	Yes	Dynamic	No	Yes	L1, E1, L5, E5a
Untargeted DFMC	No	No	Static	Advance	N/A	L1, E1, L5, E5a
Meaconing DFMC	No	No	Static	Delay	N/A	L1, E1, L5, E5a

Result Analysis
(Targeted SFMC)

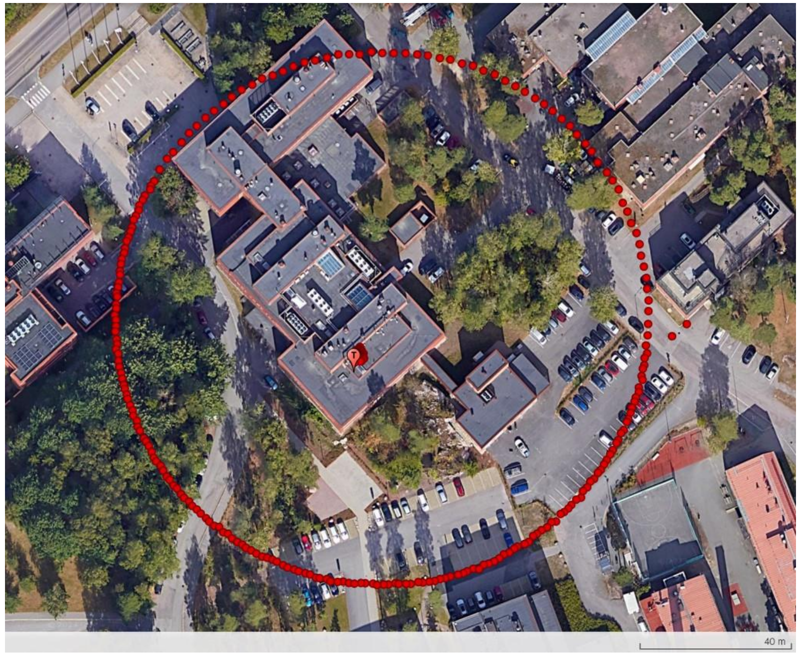
- Following the initial nominal period, the smooth transition of control over both GPS and Galileo satellites is reflected in their C/N0 values
- The intended location of the spoofing signal is clearly illustrated at the bottom of the figure. A circle with a diameter of 70 meters signifies the location intended by the spoofer



C/N0 of GPS L1



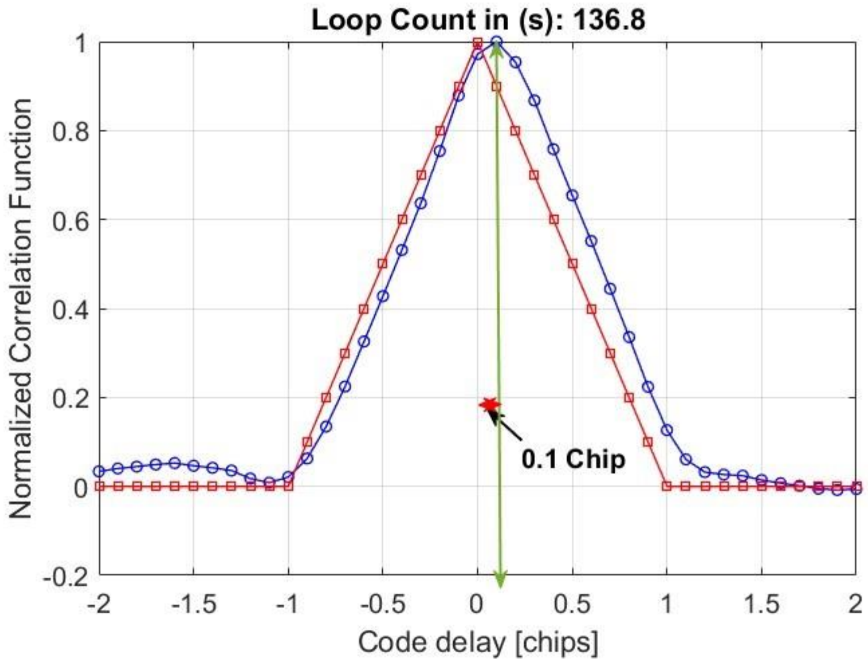
C/N0 of Galileo E1



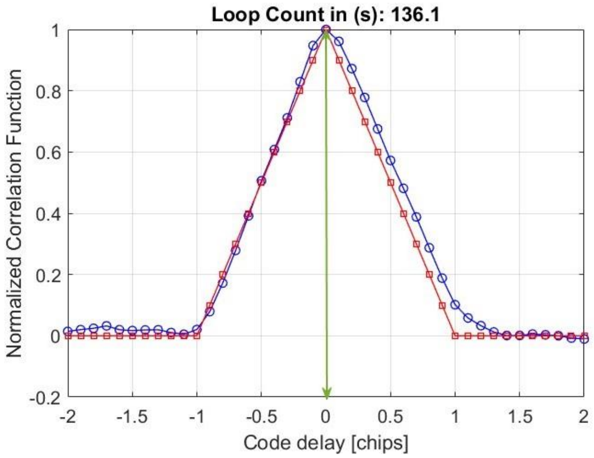
Result Analysis (Continue)

(Targeted SFMC)

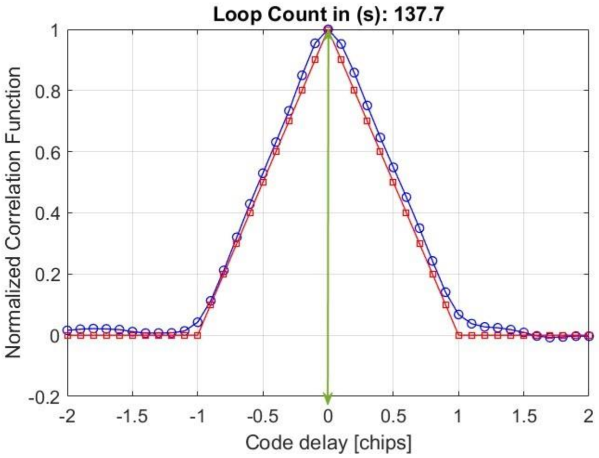
- Multi-correlator monitoring is used to further assess the smoothness of the spoofing signal with the authentic signal. 41 complex correlators are utilized with a code delay window of ±2 chips and a 0.1 chips correlator spacing
- The figures illustrate the normalized correlation function at different tracking stages of GPS PRN 7. The spoofing signal closely aligns with the authentic signal, causing only a 0.1 chips delay during the capture phase



During Capture



Before Capture



After Capture

High Accuracy Authenticated Positioning

RTK+OSNMA Performance Analysis – Results from Test Campaigns

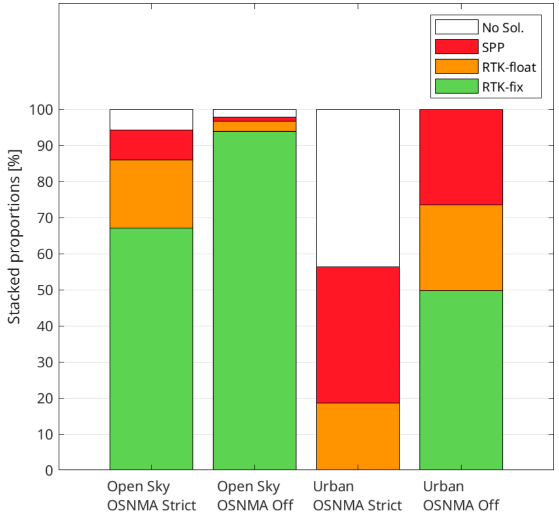
Tests in Finland

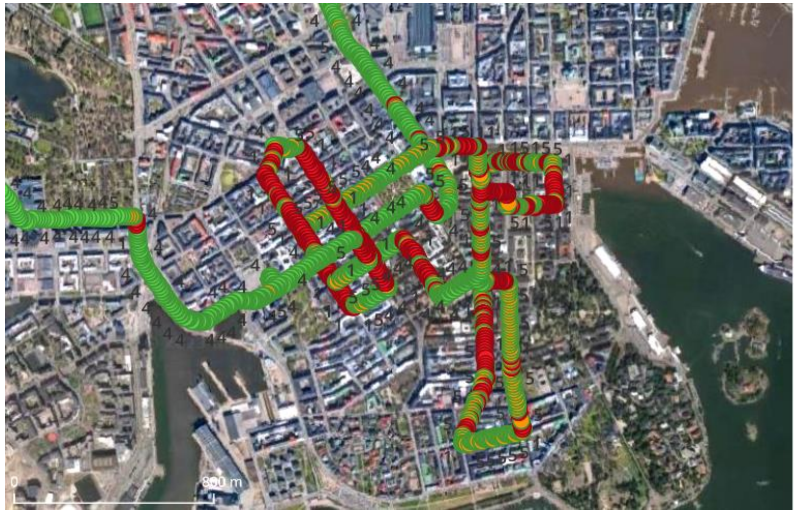
- GPS L1/L2 + Gal E1/E5a
- RTK + Standalone fallback
- Open sky and urban env.
- OSNMA in off and strict modes

High Accuracy Authenticated Positioning

RTK+OSNMA Performance Analysis – Results from Test Campaigns*

Tests in Finland





Solution types – OSNMA off

Solution types – OSNMA strict

Horizontal Accuracy
(95 Pctl.)

Env. \ OSNMA	OFF	Strict
Open Sky	0.14 m	0.75 m
Urban	10.19 m	18.47 m

Horizontal Availability
(Error < 10 cm)

Env. \ OSNMA	OFF	Strict
Open Sky	92.42%	74.10%
Urban	39.63%	4.68%

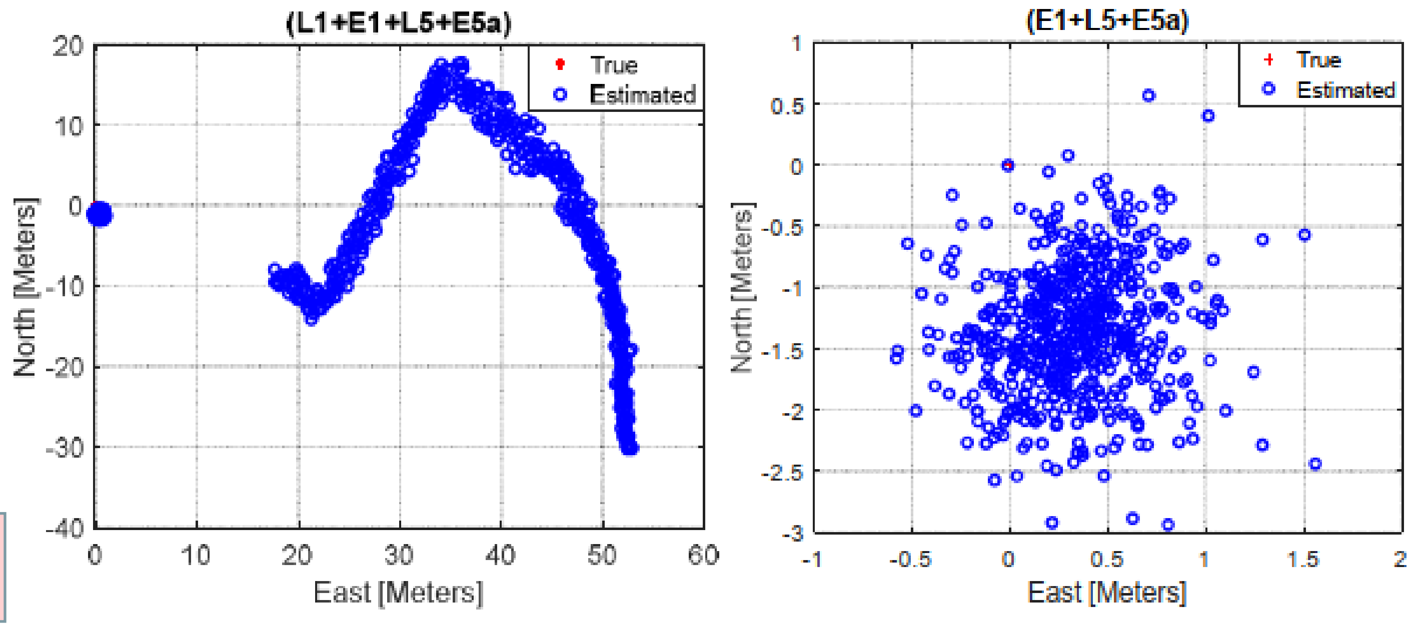
*Vallet García, José M., and M. Zahidul H. Bhuiyan. 2024. "RTK+OSNMA Positioning for Road Applications: An Experimental Performance Analysis in Finland" *Sensors* 24, no. 2: 621. https://doi.org/10.3390/s24020621

Mitigation via exploiting multi-constellation and multi-frequency diversity

- **Resilient FGI-GSRx MFMC receiver**: Intelligent signal selection based on key vulnerability matrix.

TABLE VIII. SUMMARY OF SPOOFING IMPACT ON POSITIONING ACCURACY FOR SPECIAL SPOOFING ATTACK (GPS L1 ONLY)

DUT	ε_{3D}	ε_H	σ_H	ε_V	σ_V	*Availability (%)*	*Impact*
FGI-GSRx (L1 only)	194.8	190.6	98.7	40.2	18.0	100	High
FGI-GSRx (L1+E1)	80.2	74.9	37.7	28.6	14.8	100	High
FGI-GSRx (L1+E1+L5+E5a)	39.8	37.8	18.6	12.4	6.1	100	High
FGI-GSRx (E1+L5+E5a)	4.5	1.5	0.4	4.2	0.9	100	Low
M8T	158.4	100.5	62.0	122.4	77.2	98.1	High
F9P	117.5	117.1	68.4	9.6	6.1	100	High
X5	12.9	11.4	7.4	6.1	4.1	78.1	High
Delta-3	86.7	63.4	57.3	59.1	53.6	100	High



(Left): Position solution with all available constellations, (Right): Spoofing detection-based constellation selection for position solution with FGI-GSRx

https://github.com/nlsfi/FGI-GSRx
https://doi.org/10.1017/9781108934176

Islam, S., Bhuiyan, M. Z. H., Pääkkönen, I., Saajasto, M., Mäkelä, M., and Kaasalainen, S. (2023) "Impact analysis of spoofing on different-grade GNSS receivers," IEEE/ION PLANS 2023, April 24-27, 2023, California, USA.

Recommendations on Resilient PNT: Receiver/Antenna Technologies

- Multi-constellation Multi-frequency diversity
- Modernized GNSS signals and services such as Galileo E1 OSNMA (currently under live testing phase) and Galileo E6 CAS encryption (currently under development)
- Intelligent advance algorithms at tracking and measurement layers
- 'Resilient PNT Conformance framework'* will directly influence the future design, acquisition, and deployment of resilient PNT systems at a global scale.
- Low-cost antenna array solution may improve PNT resilience in the form of interference/spoofing source detection, localization, and mitigation

* https://www.dhs.gov/sites/default/files/2022-05/22_0531_st_resilient_pnt_conformance_framework_v2.0.pdf

Recommendations on Resilient PNT: Alternate PNT / Sensor Fusion

- LEO signals and satellite constellations specifically dedicated to PNT
- Receiver specific implementation that is yet to be emerged as a commercial solution to exploit GNSS+INS+LEO+SOOP (5G, etc.) with intelligent fallback mechanism.
- Space-borne interference monitoring at LEO
- Coupling of communication and localization capabilities could be used for positioning in drones, road, in and around airports and coastal areas.

Recommendations on Resilient PNT: GNSS Performance Monitoring and Alerting Network

- A wide area GNSS threat monitoring system can be developed utilizing existing national or international continuously operated reference stations, that can simultaneously monitor all GNSS frequency bands and report to a central database in case of a vulnerability incident.
- The establishment of an international or EU-level unified interference monitoring hub to identify, detect, locate, and auto-report GNSS disruptions.
- Crowdsourced interference detection could be better utilized for GNSS interference/signal quality heatmap generation.
- Privacy issue is a big concern from a regulatory perspective, and this needs to be tackled for crowdsourced data.
- Dissemination actions among the member states need to be undertaken to increase awareness and motivation among all authoritative bodies

Advancing together

NLS
FINNISH GEOSPATIAL RESEARCH INSTITUTE
FGI